

# Securing Your Computer: General Practices

## Windows and Macintosh

This document contains the following sections:

- [Definitions](#)
  - [How to Receive Computing Alerts](#)
  - [Understanding E-mail Clients and Attachments](#)
  - [E-mail Spoofing](#)
  - [Peer to Peer File Sharing](#)
  - [How to Scan Downloaded Files](#)
  - [Create a Separate Administrator Account & Password](#)
  - [Establish a Backup Routine](#)
  - [Physical Security](#)
- 

For information related to this topic refer to:

- [Securing Your Windows XP Computer](http://www.cmu.edu/computing/doc/security/win-xp/index.html)  
(<http://www.cmu.edu/computing/doc/security/win-xp/index.html>)
- [Securing Your Windows Vista Computer](http://www.cmu.edu/computing/doc/security/vista/index.html)  
(<http://www.cmu.edu/computing/doc/security/vista/index.html>)
- [Securing Your Mac](http://www.cmu.edu/computing/doc/security/mac/index.html) (<http://www.cmu.edu/computing/doc/security/mac/index.html>)
- [Securing Your Unix Machine](http://www.cmu.edu/computing/doc/security/unix/index.html)  
(<http://www.cmu.edu/computing/doc/security/unix/index.html>)
- [Norton AntiVirus 10 for Mac OS X 10.3 and higher](http://www.cmu.edu/computing/doc/software/virus-mac/index.html)  
(<http://www.cmu.edu/computing/doc/software/virus-mac/index.html>)
- [Symantec Endpoint Protection](http://www.cmu.edu/computing/doc/software/index.html)  
(<http://www.cmu.edu/computing/doc/software/index.html>)
- [System Restore](http://www.cmu.edu/computing/doc/security/restore/index.html) (<http://www.cmu.edu/computing/doc/security/restore/index.html>)
- [Information Security Office](http://www.cmu.edu/computing/security/) (<http://www.cmu.edu/computing/security/>)
- **Frequently Asked Questions**
  - o [Peer to Peer File Sharing](http://www.cmu.edu/computing/doc/network/filesshare/faqpeer.html)  
(<http://www.cmu.edu/computing/doc/network/filesshare/faqpeer.html>)
  - o [Web and Password Security](http://www.cmu.edu/computing/doc/security/faqpassword.html)  
(<http://www.cmu.edu/computing/doc/security/faqpassword.html>)

*Last Updated: 09/08/09*

## Definitions

This document offers more indepth explanations for information included in the Securing Your Machine document.

### **Definition:** Computer Virus

Similar to a biological virus, a computer virus piggybacks on top of other programs or documents in order to become executed, infecting the machine. Viruses can be carried along via e-mail or other files that you have downloaded or transferred. Up to date anti-virus software or special removal tools are used to detect and clean viruses.

### **Definition:** Computer Worm

There are also malicious programs called worms. Worms, unlike viruses, spread by sending copies of themselves across the network, exploiting vulnerabilities in programs on other computers. Up to date anti-virus software or special removal tools are used to detect and clean worms.

### **Definition:** Computer Breakins

Breakins are attacks that specifically target your computer. Breakins can occur through a file you download and run, or via some security hole exposed through a network connection. Breakins are NOT always detectable through up to date antivirus software and typically, there is no automated clean up method. Most often it is recommended or even required that the machine be reformatted and reinstalled since determining the extent of the breakin is usually very difficult.

Today, many malicious programs are hybrids with characteristics of both viruses and worms. The program may initially infect a machine by being executed from an email attachment, but will then execute code which attempts to infect other systems via file sharing, or by exploiting vulnerabilities on other networked computers. Once it is running, the virus can infect other programs, documents or computers.

### **Definition:** File System Realtime Protection

File System Realtime Protection allows the program to automatically check all files as they are downloaded and used. This feature is turned on by default when you load the Symantec anti-virus software. However, some people disable this feature in an effort to speed up their connection. This is HIGHLY discouraged.

### **Definition:** Microsoft Updates

Microsoft updates come in three types: High Priority; Software, Optional; and Hardware, Optional.

- **High Priority** updates are absolutely critical and often fix security vulnerabilities that would allow malicious people to take control of your computer or crash it remotely. High Priority updates should be installed as soon as possible.
- **Software, Optional** updates add new features and capabilities to your existing applications. As the name suggests this update is optional.
- **Hardware, Optional** updates upgrade your device drivers to fix bugs or improve performance.

**Definition:** Things to Consider when Reading E-mail

- **How do you read your email?** Older versions of Outlook Express (Windows) are an open door to viruses and worms. We strongly urge Windows users to upgrade to Outlook (not Outlook Express) version 2003.
- **Be cautious when you receive mail with attachments.** Carnegie Mellon's mailservers are not configured to block or remove email that contains file attachments that are commonly used to spread viruses, such as .vbs, .bat, .exe, .pif and .scr files. This places more responsibility on users to exercise caution when receiving attachments.
- **Do not open attachments unless you are expecting them.** Because of the way some viruses harvest email addresses, an infected message may appear to come from someone you know. Even if a message comes from a trusted source, it may contain an infected payload. (RE: APPLICATION) HR.

**Definition:** Firewalls

A firewall is a system designed to reinforce the Security of the data flowing between two networks, the internal network and the outside network, such as the internet. All messages entering or leaving pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. Firewalls can also make your computer "invisible" to the outside world so that it doesn't become an easy target for an attacker.

**Definition:** Exceptions

An exception is a hole you open in the firewall for use by a specific application or service. This hole or set of ports allows that application or service to answer incoming connect requests from the network based on the scope of the exception. The scope defines where the allowed callers are located. Possible scope values are: any computer, subnet, and custom.

The any computer scope allows any computer on the Internet to connect to that application/service. The subnet scope allows any computer in your building (roughly speaking) to connect. The custom scope allows you to define multiple subnets (buildings) that are allowed to connect.

Unless your computer is a server, it should have very few if any exceptions.

**Definition:** Disable Unused Services

Many Windows features for operating in corporate networks are provided by specific programs that run in the background. These background programs are called Services.

Many of these Services are un-necessary on most computers and may be disabled so that malicious attackers cannot exploit security flaws in them.

Of the services listed below, the only one that may disable needed functionality is the Server service which allows you to share folders from your computer and printers that are connected to your computer. The Server service happens to be the most attacked network component of Windows and your security exposure will be reduced greatly by turning it off. If you need to share folders and printers, you should NOT disable the server service but do follow the rest of the recommendations. However, if you only need to use shared folders and printers from other servers and machines, then you can safely disable the Server service.

Service	Recommended Setting
Clipboard	Disabled
Messenger	Disabled
Machine Debug Manager	Disabled
Remote Registry	Disabled
Universal Plug and Play	Disabled
Telnet	Disabled
Alert Service	Disabled
Indexing	Disabled
NetMeeting Remote Desktop Sharing	Disabled
Routing and Remote Access	Disabled
Server Service	Disabled
Smart Card	Disabled
SSDP Discovery Service	Disabled

**Note:** In some instances, these services could be useful. In most cases, however, they are not needed, and provide potential security vulnerabilities.

**Definition:** Be Aware of the Programs you are Running

Some programs, including many of the peer-to-peer file sharing programs used to obtain music and media files, install "stealth programs" on your computer when they are installed. These programs can monitor your browsing habits, execute pop-up messages, and impair the performance of your machine. Most of the peer-to-peer programs also automatically run as servers. This can lead to problems if your machine is found to be illegally distributing copyright protected files (music, movies, television shows, or software).

There are also viruses and worms which are spread using peer-to-peer file sharing protocols. If you are going to run such programs, be sure that you know what the program is doing, and what it installs. This helps you to avoid

problems which could cause you to lose your network connection, or to need to reinstall your machine.

Do not execute software that is downloaded from the Internet unless it has been scanned for viruses. Simply visiting a compromised Web site can cause infection if certain browser vulnerabilities are not patched.

**Reminder:** [Bandwidth](#)

(<http://www.cmu.edu/computing/guideline/bandwidth.html>) guidelines that limit your traffic are in effect. Be aware of your computer's programs and report any abnormal behavior to the [Computing Services Information Security Office \(ISO\)](#) (<mailto:abuse@andrew.cmu.edu>) and the Help Center ([advisor@andrew.cmu.edu](mailto:advisor@andrew.cmu.edu) (<mailto:advisor@andrew.cmu.edu>)).

**Definition:** Common Computer Terms

These terms are provided by [Tech Encyclopedia](#) (<http://www.techweb.com/encyclopedia/>).

- **Ports** - In a TCP/IP-based network such as the Internet, it is a number assigned to an application running in the computer. See Common Ports list below.
- **NetBIOS** - The native networking protocol in DOS and Windows networks.
- **MAC Address** - The unique serial number burned into Ethernet adapters that identifies that network card from all others.
- **Trojan Horse Program** - A program that appears legitimate, but performs some illicit activity when it is run.
- **Worm** - A destructive program that replicates itself throughout disk and memory, using up the computer's resources.
- **Virus** - Software used to infect a computer. After the virus code is written, it is buried within an existing program.

**Common Ports:**

20 FTP data (File Transfer Protocol)  
21 FTP (File Transfer Protocol)  
22 SSH (Secure Shell)  
23 Telnet  
25 SMTP (Send Mail Transfer Protocol)  
43 whois  
53 DNS (Domain Name Service)  
68 DHCP (Dynamic Host Control Protocol)  
79 Finger  
80 HTTP (HyperText Transfer Protocol)  
110 POP3 (Post Office Protocol, version 3)  
115 SFTP (Secure File Transfer Protocol)  
119 NNTP (Network New Transfer Protocol)  
123 NTP (Network Time Protocol)  
137 NetBIOS-ns  
138 NetBIOS-dgm

139 NetBIOS  
143 IMAP (Internet Message Access Protocol)  
161 SNMP (Simple Network Management Protocol)  
194 IRC (Internet Relay Chat)  
220 IMAP3 (Internet Message Access Protocol 3)  
389 LDAP (Lightweight Directory Access Protocol)  
443 SSL (Secure Socket Layer)  
445 SMB (NetBIOS over TCP)  
666 Doom  
993 SIMAP (Secure Internet Message Access Protocol)  
995 SPOP (Secure Post Office Protocol)  
1243 SubSeven (Trojan - security risk!)  
1352 Lotus Notes  
1433 Microsoft SQL Server  
1494 Citrix ICA Protocol  
1521 Oracle SQL  
1604 Citrix ICA / Microsoft Terminal Server  
2049 NFS (Network File System)  
3306 mySQL  
4000 ICQ  
5010 Yahoo! Messenger  
5190 AOL Instant Messenger  
5632 PCAnywhere  
5800 VNC  
5900 VNC  
6000 X Windowing System  
6699 Napster  
6776 SubSeven (Trojan - security risk!)  
7070 RealServer / QuickTime  
7778 Unreal  
8080 HTTP  
26000 Quake  
27010 Half-Life  
27960 Quake III  
31337 BackOrifice (Trojan - security risk!)

## How to Receive Computing Alerts

Computing Services has chosen three methods to communicate security alerts: the compserv-security mailing list, the official.computing-news postings, and the [Computing Services headline portlet \(https://my.cmu.edu/\)](https://my.cmu.edu/). Select the communication method that best suits you and commit to reading it on a regular basis.

For more information, visit the [Computing Services Security Alert Notifications \(http://www.cmu.edu/computing/news/getnews/index.html\)](http://www.cmu.edu/computing/news/getnews/index.html) web page.

*Last Updated: 04/15/08*

# Understanding E-mail Clients and Attachments

## E-mail Clients

Mail clients are the applications you use to read or send your mail messages. Carnegie Mellon uses the Cyrus electronic mail and bulletin board system. To help you choose a supported email client, we recommend reading the *Supported Mail Clients* section of the *Email Overview at Carnegie Mellon* (<http://www.cmu.edu/computing/email/clients.html>) document.

## Securing Your Email Client

Computing Services does not allow clear-text authentication to servers on campus. This means that any email client used with Computing Services' email servers **MUST** be configured to use an authentication method that provides encryption of the users' password.

## Opening Attachments

Because of the way some viruses harvest e-mail addresses, an infected message may appear to come from someone you know, or may even show your name in the "From" line. Be extremely cautious and check with the sender (even if you know them) before you open e-mail attachments. It's less of an inconvenience than cleaning up after an infection. There are a number of things to consider when reading your e-mail messages. For more information, see *Securing Your Machine: Definitions*.

Important Note: Computing Services will NEVER send a security announcement e-mail message that contains an attachment.

*Last Updated: 02/01/07*

## E-mail Spoofing

Many e-mail viruses use a technique known as "spoofing" by which the worm randomly selects an address it finds on an infected computer. The worm uses this address as the "From" address when it performs its mass-mailing routine. Numerous cases have been reported in which users of uninfected computers received complaints that they sent an infected message to another individual.

For example, Linda Anderson is using a computer infected with W32.Sobig.F@mm. Linda is neither using an antivirus program nor has the current virus definitions. When W32.Sobig.F@mm performs its email routine, it finds the email address of Harold Logan. The worm inserts Harold's email address into the "From" portion of an infected message, which it then sends to Janet Bishop. Then, Janet contacts Harold and complains that he sent her an infected message; however, when Harold scans his computer, his antivirus program does not find anything, because his computer is not infected.

*Last Updated: 02/01/07*

## Peer to Peer File Sharing

Peer to peer file sharing is the practice of downloading files from another “peer” workstation. This practice can be used for legal or illegal purposes. For additional information on Peer to Peer File Sharing, refer to [Peer to Peer and P2P File Sharing \(http://www.cmu.edu/computing/doc/network/filesshare/index.html\)](http://www.cmu.edu/computing/doc/network/filesshare/index.html) .

*Last Updated: 09/08/09*

## How to Scan Downloaded Files

Do not execute software that is downloaded from the Internet unless it has been scanned for viruses. Simply visiting a compromised Web site can cause infection if certain browser vulnerabilities are not patched. For more information, see [Securing Your Machine: Definitions](#).

### Windows

Before opening any file you've downloaded you should **right-click the file** and select the option **Scan for Viruses**. A practical solution is to create a folder on your C: drive called Downloads and save everything into that. This gives you quick and easy access to your files and you'll always remember where they are saved.

Once you've put your file into Downloads, you can right click it and scan it for viruses before opening it. NEVER open files from people or sources you're unfamiliar with (whether they come from a website or an e-mail) and always **scan them first!**

### Macintosh

Before downloading any files, you should have Norton Auto-Protect turned on. A practical solution is to create a folder on your hard drive called **Downloads** and save everything to that. This gives you quick and easy access to your files and you'll always remember where they are saved.

Once you've saved your files into Downloads, you can run Norton Anti-Virus and scan the folder for viruses before opening it. NEVER open files from people or sources you're unfamiliar with (whether they come from a website or an e-mail) and always **scan them first!**

*Last Updated: 02/01/07*

## Create a Separate Administrator Account

Most of your daily computer activity does not require admin access. Normally you only need admin access to install software and make critical configuration changes. However, an admin account can also be used to override all security setting. By using a normal user account for daily work you limit the damage a virus or malicious attacker can inflict.

For complete instructions on creating a separate administrator account refer to the following documentation:

- **Windows XP** - Secure Your Accounts section of the <http://www.cmu.edu/computing/doc/security/win-xp/index.html> *Securing Your Windows XP Computer* (<http://www.cmu.edu/computing/doc/security/win-xp/index.html>) document.
- **Windows Vista** - Secure Your Accounts section of the *Securing Your Windows Vista Computer* (<http://www.cmu.edu/computing/doc/security/vista/index.html>) document.
- **Macintosh** - Advanced section of the *Securing Your Mac* (<http://www.cmu.edu/computing/doc/security/mac/index.html>) document.

## Select a Secure Administrator Password

Selecting a secure administrator password for your machine is important. Having a blank administrator password, or one which is easy to crack, is asking for trouble. For help with selecting a password read the *Select a Secure Password* section of the *Managing Your Andrew Password* (<http://www.cmu.edu/computing/doc/accounts/passwords/index.html>) document.

*Last Updated: 02/01/07*

## **Establish a Backup Routine**

It's easy to forget about keeping a backup of your important data. In the event of hardware failure or compromise of the computer your hard work may be gone forever.

For help with establishing a backup routine, refer to [Preparing for Recovery.](http://www.cmu.edu/computing/doc/os/recovery/prepare.html)  
(<http://www.cmu.edu/computing/doc/os/recovery/prepare.html>)

*Last Updated: 09/21/09*

## Physical Security

When leaving a computer for a short or extended period of time, either log out or lock the machine. You should also enable a screen saver password. For more information refer to the following documentation:

- **Windows XP** - *Enable a Screen Saver Password* section of the *Securing Your Windows XP Computer* (<http://www.cmu.edu/computing/doc/security/win-xp/index.html>) document.
- **Windows Vista** - *Enable a Screen Saver Password* section of the *Securing Your Windows Vista Computer* (<http://www.cmu.edu/computing/doc/security/vista/index.html>) document.
- **Macintosh** - *Set a Screen Saver* section of the *Securing Your Mac* (<http://www.cmu.edu/computing/doc/security/mac/index.html>) document.

*Last Updated: 02/01/07*